25

CLAIMS

1. Method for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol, wherein said wireless communication apparatus has memory means including a separate unit comprising information to control the access of the wireless communication apparatus through a wireless communication network connected to said data communication apparatus, comprising the following steps:

connecting said wireless communication apparatus to the separate unit,

accessing the wireless communication network connected to said data communication apparatus

the wireless communication apparatus transmits a request to the data communication apparatus to establish a connection, said request comprising information of which pre-defined algorithm(s) the wireless communication apparatus supports,

upon reception of said request, the data communication apparatus chooses at least one algorithm associated with a public and a private key, and transmits a message back to the wireless communication apparatus, said message comprising the public key and information about which algorithm the data communication apparatus has chosen,

upon reception of the message, comprising the public key, the wireless communication apparatus generates a master secret code, and calculates a signature based on the chosen algorithm, the public key and the master secret code, and transmits a response to the data communication apparatus, said response comprising the calculated signature,

upon reception of the respond comprising the signature, the data communication apparatus calculates the master secret code based on the

chosen algorithm, the signature received and the private key, and establish a secure connection to the wireless communication apparatus, and
saving said master secret code on said memory means and in the data communication apparatus, in order to re-establish the connection at a later occasion.

2. A method according to claim 1, and comprising a step of saving said master secret under a pre-defined time.

3. A method according to claim 1 or 2, and comprising a step of re-establishing the connection by
transmitting a request from the wireless communication apparatus to the data communication apparatus, said request comprising the calculated signature based on the chosen algorithm, the public key and the stored secret key, and
upon reception of the request, the data communication apparatus calculates the master secret code based on the chosen algorithm, the signature received, and the private key, and, establish a secure connection to the wireless communication apparatus.

4. A method according to claim 1, 2, or 3, and comprising a step of providing said separate unit in a smart card.

5. Wireless communication apparatus for establishing a secure connection to a data communication apparatus based on a wireless application protocol, said wireless communication apparatus comprising:
communication means for establishing a connection to a wireless communication network connected to said data communication apparatus,
memory means including a separate unit provided with information to control the access of the data communication apparatus through the wireless communication network,

means for generating a master secret code

control means arranged to use a pre-defined algorithm(s) for generating a signature based on said master secret code and a public key received from said data communication apparatus, for use when the wireless communication apparatus establishes a secure connection to the data communication apparatus,

said memory means comprising a secure database for storing at least one master secret code and/or at least one signature related to one or more data communication apparatus, in order to re-establish a secure connection to a data communication apparatus.

6. A wireless communication apparatus according to claim 5, having its memory means exchangeable.

7. Wireless communication apparatus according to claim 5 or 6 wherein the master secret code is stored on the separate unit.

8. Wireless communication apparatus according to any one of claims 5 to 7 wherein the signature is stored on the separate unit.

9. Wireless communication apparatus according to any one of claims 5 to 8 wherein the master secret code is generated on the separate unit.

10. Wireless communication apparatus according to any one of claims 5 to 9 wherein the signature is generated on the separate unit.

11. Wireless communication apparatus according to any one of claims 5 to 10 wherein the separate unit comprises a smart card.

25

12. An apparatus according to claim 11 wherein the smart card is a subscriber identity module.

13. A smart card according to claims 11 or 12.

14. A wireless communication apparatus according to any one of claims 5 to 12 without the smart card of claim 13.

15. Memory card for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol, arranged to be connected to contact means, provided on said wireless communication apparatus, for providing information from the memory card to the wireless communication apparatus upon establishing a secure session to a data communication apparatus, said information is arranged to control the access of the data communication apparatus through a wireless communication network, and to save a calculated master secret related to one or more data communication apparatus, in order to re-establish a secure connection to a data communication apparatus.

16. A memory card according to claim 15, further comprising encryption means for encrypting the master secret, which is to be used as a signature for the wireless communication apparatus when it is establishing a secure connection.

17. A memory card according to claim 15 or 16, comprising a secure database provided with at least one master secret code and/or at least one signature related to one or more data communication apparatus, in order to re-establish a secure connection to a data communication apparatus.

18. A memory card according to claim 15, 16, or 17, is provided on a smart card.

19. System for establishing a secure connection when using a wireless application protocol, comprising:

a data communication apparatus based on the wireless application protocol,

a wireless communication network, connected to said data communication apparatus,

a wireless communication apparatus having memory means including a separate unit comprising information to control the access of the wireless communication apparatus through the wireless communication network, wherein

the wireless communication apparatus is arranged to transmit a request to the data communication apparatus to establish a connection, said request comprising information of which pre-defined algorithm(s) the wireless communication apparatus supports,

upon reception of said request, the data communication apparatus is arranged to choose at least one algorithm, associated with a public key and a private key, and to transmit a message back to the wireless communication apparatus, said message comprising the public key and information about which algorithm the data communication apparatus will choose,

upon reception of said message, comprising the public key, the wireless communication apparatus is arranged to generate a master secret code, to calculate a signature based on the chosen algorithm, the public key and the master secret code, and to transmit a respond to the data communication apparatus, said respond comprising the calculated signature,

upon reception of the respond comprising the signature, the data communication apparatus is arranged to calculate the master secret code based on the chosen algorithm, the signature received, and the private key,

and, thus establish a secure connection to the wireless communication apparatus, and

said memory means being arranged to save said master secret code, in order to re-establish the connection at a later occasion.

20. A system according to claim 19, said master secret is arranged to be saved under a pre-defined time.

21. A system according to claim 19, or 20, said memory means is a smart card.

22. A wireless communication apparatus for establishing a secure connection to a data communication apparatus through a wireless network based on a wireless application protocol, said wireless communication apparatus comprising:

means for establishing a connection with the data communication apparatus through the wireless network

means for retrieving access information including which of a set of pre-define algorithms is supported, for transmission to the data communication apparatus;

means for processing information including a public key and the selection of one of the supported algorithms received from the data communication apparatus for storage;

means for retrieving a signature based on a generated master secret code and the public key received from the data communication apparatus; and

means for utilising the signature and/or the master secret key during communication with the data communication apparatus in order to re-establish a secure connection.

23. A memory card for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol comprising contact means for cooperation with the wireless communication apparatus

a memory for storing a master secret code associated with the data communication apparatus and responsive to a request from the wireless communication apparatus to provide such code for utilisation of the master secret key during communication with the data communication apparatus in order to re-establish a secure connection.

24. Wireless communication apparatus for establishing a secure connection to a data communication apparatus based on a wireless application protocol, said wireless communication apparatus comprising:

communication means for establishing a connection to a wireless communication network connected to said data communication apparatus,

memory means provided with information to control the access of the data communication apparatus through the wireless communication network upon establishing a secure session to a data communication apparatus,

reading means for reading information received from the data communication apparatus and the information provided on said memory means,

means for generating a master secret code,

control means arranged to use a pre-defined algorithm(s) for generating a signature based on said master secret code and a public key received from said data communication apparatus, which is to be used when the wireless communication apparatus is going to establish a secure connection to the data communication apparatus, and

said reading means comprising a secure database provided with at least one master secret code and/or at least one signature related to one or more data communication apparatus, in order to re-establish a secure connection to a data communication apparatus.